Requested Patent: JP2001013870A

Title:

METHOD OF COMMON KEY ENCIPHERING OR DECIPHERING, AND RECORDING MEDIUM WITH COMMON KEY CIPHERING OR DECIPHERING PROGRAM RECORDED THEREON ;

Abstracted Patent: JP2001013870 ;

Publication Date: 2001-01-19 ;

Inventor(s): IMOTO AKIO ;

Applicant(s): NEC CORP ;

Application Number: JP19990184453 19990629 ;

Priority Number(s): ;

IPC Classification: G09C1/00; H04L9/06 ;

Equivalents: ;

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a common key ciphering method virtually disabling a known plaintext attack and a selected plaintext attack.SOLUTION: The disclosed common key enciphering method enciphers a plaintext by preparing a table of random digits and a reading mechanism 1, an indirect index array 2, and a four-dimensional matrix 4 with constant coefficients beforehand, deciding display start positions of each step of the table of random digits from a secret key 6, calculating (p+q) pieces of original maps by the table of random digits and the reading mechanism 1 every time m-bytes of character string is taken out of a plaintext, generating a 1st indirect index array presenting a composited map of the p-pieces of original lamp numbers and a 2nd indirect index array presenting a composited map of the q-pieces of original map numbers, converting the character string taken out of the plaintext data by the 1st indirect index array, converting the character string of this conversion result by integrating it with m-dimensional matrix with constant coefficients, and storing in the ciphertext a character string obtained by converting the character string of the conversion result by the 2nd indirect index array.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－13870
（P2001－13870A）
(43)公開日　平成13年１月19日(2001.1.19)

(51)Int.Cl.'	識別記号	FI	テーマコード(参考)
G09C 1/00	610	G09C 1/00	610Z 5J104
H04L 9/06		H04L 9/00	611Z

審査請求　有　請求項の数８　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－184453

(22)出願日　平成11年６月29日(1999.6.29)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　井本　明夫
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100099830
弁理士　西村　征生

Ｆターム(参考)　5J104 AA01 JA13 JA15 NA10

(54)【発明の名称】　共通鍵暗号化又は復号化方法と、共通鍵暗号化又は復号化プログラムを記録した記憶媒体

(57)【要約】
【課題】　既知平文攻撃並びに選択平文攻撃を事実上不可能とする、共通鍵暗号化方法を提供する。
【解決手段】　開示される共通鍵暗号化方法は、乱数表と読み出し機構１と、間接指標配列２と、定数係数の４次行列４を予め用意し、秘密鍵６から乱数表の各段の表示開始位置を決定して、平文データからｍバイトの文字列を取り出すごとに、乱数表と読み出し機構１によって、（ｐ＋ｑ）個の原写像の番号を算出し、ｐ個の原写像番号の合成写像を表す第１の間接指標配列と、ｑ個の原写像番号の合成写像を表す第２の間接指標配列とを作成して、平文データから取り出された文字列を第１の間接指標配列で変換し、変換結果の文字列を定数係数のｍ次行列との積算で変換し、この変換結果の文字列を第２の間接指標配列で変換して得た文字列を、暗文データ中に格納することによって、平文の暗号化を行う。

1

対象文字が89種の場合の文字―数値間の対応の例

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
&	'	(	)	*	+	,	−	.	／	0	1	2	3	4	5
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
6	7	8	9	:	;	<	=	>	?	@	A	B	C	D	E
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
V	W	X	Y	Z	[	¥	]	^	_	`	a	b	c	d	e
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
80	81	82	83	84	85	86	87	88							
v	w	x	y	z	{	|	}	～							

【特許請求の範囲】

【請求項１】　長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数のｍ次行列とを予め用意し、

秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、

平文データからｍバイトの文字列を取り出すごとに、前記乱数表と読み出し機構によって、前記（ｐ＋ｑ）個の原写像の番号の算出を行い、該（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号に示される原写像の合成写像を表す第１の間接指標配列と、前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号に示される原写像の合成写像を表す第２の間接指標配列とを作成して、前記平文データから取り出された文字列を前記第１の間接指標配列で変換し、次に該変換結果の文字列を前記定数係数のｍ次行列との積算で変換し、さらに該変換結果の文字列を前記第２の間接指標配列で変換して得た文字列を、暗文データ中のｍバイトの文字列として暗文データに格納する処理を、前記平文データからのｍバイトの文字列の読み出しごとに、前記乱数表の各段の表示位置を１個ずつずらしながら繰り返すことによって、平文の暗号化を行うことを特徴とする共通鍵暗号化方法。

【請求項２】　長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数のｍ次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、

暗文データからｍバイトの文字列を取り出すごとに、前記乱数表と読み出し機構によって、前記（ｐ＋ｑ）個の原写像の番号の算出を行い、該（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第１の間接指標配列と、前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第２の間接指標配列とを作成して、前記暗文データから取り出された文字列を前記第２の間接指標配列で変換し、次に該変換結果の文字列を前記定数係数のｍ次行列の逆行列との積算で変換し、さらに該変換結果の文字列を前記第１の間接指標配列で変換して得た文字列を、平文データ中のｍバイトの文字列として平文データに格納する処理を、前記暗文データからのｍバイトの文字列の読み出しごとに、前記乱数表の各段の表示位置を暗号化時と逆方向に１個ずつずらしながら繰り返すことによって、暗文の復号化を行うことを特徴とする共通鍵復号化方法。

【請求項３】　長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数のｍ次行列とを予め用意し、

秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、

平文データからｍバイトの所定数の要素分のベクトルを取り出すごとに、前記乱数表と読み出し機構によって、前記要素数回分の読み出しと前記（ｐ＋ｑ）個の原写像の番号の算出を行って、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号を第１の作業ベクトルに格納するとともに、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号を第２の作業ベクトルに格納し、前記平文データから取り出したベクトルの各要素を、前記第１の作業ベクトルの各要素に含まれる、前記ｐ個の原写像番号が指し示す原写像を用いて変換し、次に該変換結果のベクトルの各要素を前記定数係数のｍ次行列との積算で変換し、さらに該変換結果のベクトルの各要素を、前記第２の作業ベクトルの各要素に含まれる、前記ｑ個の原写像番号が指し示す原写像を用いて変換して得たベクトルを、暗文データ中のｍバイトの所定数の要素分のベクトルとして暗文データに格納する処理を、平文データからのｍバイトの所定数の要素分のベクトルの読み出しごとに、前記乱数表の各段の表示位置を１個ずつずらしながら繰り返すことによって、平文の暗号化を行うことを特徴とする共通鍵暗号化方法。

【請求項４】　長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数のｍ次行列の逆行列とを予め用意し、

秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、

暗文データからｍバイトの所定数の要素分のベクトルを取り出すごとに、前記乱数表と読み出し機構によって、前記要素数回分の読み出しと前記（ｐ＋ｑ）個の原写像番号の算出を行って、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号を暗号化時と逆順に第１の作業ベクトルに格納するとともに、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号を暗号化時と逆順に第２の作業ベクトルに格納し、前記暗文データから取り出したベクトルの各要素を、前記第２の作業ベクトルの各要素に含まれる、前記ｑ個の原写像番号が指し示す原写像の逆写像を用いて変換し、次に該変換結果のベクトルの各要素を前記定数係数のｍ次行列の逆行列との積算で変換し、さらに該変換結果のベクトルの各要素を、前記第１の作業ベクトルの各要素に含まれる、前記ｐ個の原写像番号が指し示す原写像の逆写像を用いて変換して得たベクトルを、平文データ中のｍバイトの所定数の要素分のベクトルとして平文データに格納する処理を、暗文データからのｍバイトの所定数の要素分のベクトルの読み出しごとに、前記乱数表の各段の表示位置を暗号化時と逆方向に１個ずつず

らしながら繰り返すことによって、暗文の復号化を行うことを特徴とする共通鍵復号化方法。

【請求項5】　請求項1記載の共通鍵暗号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき（p＋q）個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数のm次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データからmバイトの文字列を取り出すごとに、前記乱数表と読み出し機構によって、前記（p＋q）個の原写像の番号の算出を行い、該（p＋q）個の原写像番号中のp個の原写像番号に示される原写像の合成写像を表す第1の間接指標配列と、前記（p＋q）個の原写像番号中のq個の原写像番号に示される原写像の合成写像を表す第2の間接指標配列とを作成して、前記平文データから取り出された文字列を前記第1の間接指標配列で変換し、次に該変換結果の文字列を前記定数係数のm次行列との積算で変換し、さらに該変換結果の文字列を前記第2の間接指標配列で変換して得た文字列を、暗文データ中のmバイトの文字列として暗文データに格納する処理を、前記平文データからのmバイトの文字列の読み出しごとに、前記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うプログラムを記録したことを特徴とする共通鍵暗号化プログラムを記録した記憶媒体。

【請求項6】　請求項2記載の共通鍵復号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき（p＋q）個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数のm次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データからmバイトの文字列を取り出すごとに、前記乱数表と読み出し機構によって、前記（p＋q）個の原写像の番号の算出を行い、該（p＋q）個の原写像番号中のp個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第1の間接指標配列と、前記（p＋q）個の原写像番号中のq個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第2の間接指標配列とを作成して、前記暗文データから取り出された文字列を前記第2の間接指標配列で変換し、次に該変換結果の文字列を前記定数係数のm次行列の逆行列との積算で変換し、さらに該変換結果の文字列を前記第1の間接指標配列で変換して得た文字列を、平文データ中のmバイトの文字列として平文データに格納する処理を、前記暗文データからのmバイトの文字列の読み出しごとに、前記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復号化を行うプログラムを記録したことを特徴とする共通鍵復号化プログラムを記録した記憶媒体。

【請求項7】　請求項3記載の共通鍵暗号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき（p＋q）個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数のm次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データからmバイトの所定数の要素分のベクトルを取り出すごとに、前記乱数表と読み出し機構によって、前記要素数回分の読み出しと前記（p＋q）個の原写像の番号の算出を行って、要素ごとに使用する前記（p＋q）個の原写像番号中のp個の原写像番号を第1の作業ベクトルに格納するとともに、要素ごとに使用する前記（p＋q）個の原写像番号中のq個の原写像番号を第2の作業ベクトルに格納し、前記平文データから取り出したベクトルの各要素を、前記第1の作業ベクトルの各要素に含まれる、前記p個の原写像番号が指し示す原写像を用いて変換し、次に該変換結果のベクトルの各要素を前記定数係数のm次行列との積算で変換し、さらに該変換結果のベクトルの各要素を、前記第2の作業ベクトルの各要素に含まれる、前記q個の原写像番号が指し示す原写像を用いて変換して得たベクトルを、暗文データ中のmバイトの所定数の要素分のベクトルとして暗文データに格納する処理を、平文データからのmバイトの所定数の要素分のベクトルの読み出しごとに、前記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うプログラムを記録したことを特徴とする共通鍵暗号化プログラムを記録した記憶媒体。

【請求項8】　請求項4記載の共通鍵復号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき（p＋q）個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数のm次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データからmバイトの所定数の要素分のベクトルを取り出すごとに、前記乱数表と読み出し機構によって、前記要素数回分の読み出しと前記（p＋q）個の原写像の番号の算出を行って、要素ごとに使用する前記（p＋q）個の原写像番号中のp個の原写像番号を暗号化時と逆順に第1の作業ベクトルに格納するとともに、要素ごとに使用する前記（p＋q）個の原写像番号中のq個の原写像番号を暗号化時と逆順に第2の作業ベクトルに格納し、前記暗文データから取り出したベクトルの各要素を、前記第2の作業ベクトルの各要素に含まれる、前記q個の原写像番号が指し示す原写像の逆写像を用いて変換し、次に該変換結果のベクト

ルの各要素を前記定数係数のm次行列の逆行列との積算で変換し、さらに該変換結果のベクトルの各要素を、前記第1の作業ベクトルの各要素に含まれる、前記p個の原写像番号が指し示す原写像の逆写像を用いて変換して得たベクトルを、平文データ中のmバイトの所定数の要素分のベクトルとして平文データに格納する処理を、暗文データからのmバイトの所定数の要素分のベクトルの読み出しごとに、前記乱数表の各段の表示位置を暗号化時と逆方向に1個ずつずらしながら繰り返すことによって、暗文の復号化を行うプログラムを記録したことを特徴とする共通鍵復号化プログラムを記録した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化処理と復号化処理とに共通の秘密鍵を用いる、共通鍵暗号化又は復号化方法並びに共通鍵暗号化又は復号化プログラムを記録した記憶媒体に関する。

【0002】

【従来の技術】従来、この種の暗号化方式は、秘密鍵の内容を知らずに、暗号文に対して解読を試みる攻撃者に対して、暗号化されたデータの安全性を確保することを目的として用いられている。例えば、ブロック型暗号化方式としては、現在、米国において標準化されている暗号化規格である、DES (Data Encryption Standard) 暗号によるものが、広く使用されている。しかしながら、DESでは、選択平文攻撃によって、差分解析法と呼ばれる手段で解読され、また、既知平文攻撃によって、線形解読法と呼ばれる手段で解読される危険がある。これは、DESでは、転置以外には、排他的論理和という、線形の性質を持つ変換しか行っていないためである。

【0003】また、DESは、計算機上のプログラムとしては、処理が遅いが、これによって、攻撃者が専用のハードウェアを用いた場合に、攻撃者だけが有利になって、利用者が不利になるという欠点につながる。これは、DESは、転置及びビットごとの排他的論理和という、計算機上では実行速度の遅い処理を多用しているためである。これに対して、特開平10-123949号（特願平9-217299号）公報には、DES暗号を改良して、差分解析に対して安全性を強化する技術が開示されている。しかしながら、この従来技術によっても、依然として、計算機上のプログラムとしては、処理が遅いという問題が残っている。これは、この従来技術においても、やはり、ビット転置という、計算機上では実行速度の遅い処理が多用されているためである。

【0004】一方、別の暗号化方式として、ストリーム型暗号化方式がある。例えば、特開平9-288565号（特願平8-99985号）公報においては、カオス軌道に沿った実数値の乱数列を生成して使用する技術が開示されている。しかしながら、この従来技術では、アーキテクチャの異なる複数の計算機上で、同じ動作を保証することが困難であるという問題がある。これは、実数値の乱数列を、実数演算の繰り返しによって算出するので、計算機のアーキテクチャの僅かな違いによって、発生する乱数列が異なるものになってしまうことがあるためである。また、上記の従来技術では、乱数列が短周期に陥る危険性に関して、このような危険の回避を保証できないという問題がある。これは、カオスを発生する自励系の実数演算では、周期点を発見することが難しい反面、短周期に陥っていないことの保証もしていないためである。

【0005】

【発明が解決しようとする課題】この発明は、上述の事情に鑑みてなされたものであって、暗号化処理と復号化処理とに共通の鍵を用いる、共通鍵暗号化方式であって、既知平文攻撃並びに選択平文攻撃を、事実上不可能にする、共通鍵暗号化又は復号化方法並びに共通鍵暗号化又は復号化プログラムを記録した記憶媒体を提供することを目的としている。

【0006】

【課題を解決するための手段】上記課題を解決するため、請求項1記載の発明は、共通鍵暗号化方法に係り、長周期の乱数表と、該乱数表の表示値に基づき（p+q）個（p，qは任意の自然数。以下、省略）の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数のm次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データからmバイトの文字列を取り出すごとに、上記乱数表と読み出し機構によって、上記（p+q）個の原写像の番号の算出を行い、該（p+q）個の原写像番号中のp個の原写像番号に示される原写像の合成写像を表す第1の間接指標配列と、前記（p+q）個の原写像番号中のq個の原写像番号に示される原写像の合成写像を表す第2の間接指標配列とを作成して、上記平文データから取り出された文字列を上記第1の間接指標配列で変換し、次に該変換結果の文字列を上記定数係数のm次行列との積算で変換し、さらに該変換結果の文字列を上記第2の間接指標配列で変換して得た文字列を、暗文データ中のmバイトの文字列として暗文データに格納する処理を、上記平文データからのmバイトの文字列の読み出しごとに、上記乱数表の各段の表示位置を1個ずつずらしながら繰り返すことによって、平文の暗号化を行うことを特徴としている。

【0007】また、請求項2記載の発明は、共通鍵復号化方法に係り、長周期の乱数表と、該乱数表の表示値に基づき（p+q）個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数のm次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データからmバイトの文字列

を取り出すごとに、上記乱数表と読み出し機構によって、上記（ｐ＋ｑ）個の原写像の番号の算出を行い、該（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第１の間接指標配列と、前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第２の間接指標配列とを作成して、上記暗文データから取り出された文字列を上記第２の間接指標配列で変換し、次に該変換結果の文字列を上記定数係数のｍ次行列の逆行列との積算で変換し、さらに該変換結果の文字列を上記第１の間接指標配列で変換して得た文字列を、平文データ中のｍバイトの文字列として平文データに格納する処理を、上記暗文データからのｍバイトの文字列の読み出しごとに、上記乱数表の各段の表示位置を暗号化時と逆方向に１個ずつずらしながら繰り返すことによって、暗文の復号化を行うことを特徴としている。

【０００８】また、請求項３記載の発明は、共通鍵暗号化方法に係り、長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数のｍ次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データからｍバイトの所定数の要素分のベクトルを取り出すごとに、上記乱数表と読み出し機構によって、上記要素数回分の読み出しと上記（ｐ＋ｑ）個の原写像の番号の算出を行って、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号を第１の作業ベクトルに格納するとともに、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号を第２の作業ベクトルに格納し、上記平文データから取り出したベクトルの各要素を、上記第１の作業ベクトルの各要素に含まれる、上記第ｐ個の原写像番号が指し示す原写像を用いて変換し、次に該変換結果のベクトルの各要素を上記定数係数のｍ次行列との積算で変換し、さらに該変換結果のベクトルの各要素を、上記第２の作業ベクトルの各要素に含まれる、上記第ｑ個の原写像番号が指し示す原写像を用いて変換して得たベクトルを、暗文データ中のｍバイトの所定数の要素分のベクトルとして暗文データに格納する処理を、平文データからのｍバイトの所定数の要素分のベクトルの読み出しごとに、上記乱数表の各段の表示位置を１個ずつずらしながら繰り返すことによって、平文の暗号化を行うことを特徴としている。

【０００９】また、請求項４記載の発明は、共通鍵復号化方法に係り、長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数のｍ次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データからｍバイトの所定数の要素分のベクトルを取り出すごとに、上記乱数表と読み出し機構によって、上記要素数回分の読み出しと上記（ｐ＋ｑ）個の原写像の番号の算出を行って、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号を暗号化時と逆順に第１の作業ベクトルに格納するとともに、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号を暗号化時と逆順に第２の作業ベクトルに格納し、上記暗文データから取り出したベクトルの各要素を、上記第２の作業ベクトルの各要素に含まれる、上記ｑ個の原写像番号が指し示す原写像の逆写像を用いて変換し、次に該変換結果のベクトルの各要素を上記定数係数のｍ次行列の逆行列との積算で変換し、さらに該変換結果のベクトルの各要素を、上記第１の作業ベクトルの各要素に含まれる、上記ｐ個の原写像番号が指し示す原写像の逆写像を用いて変換して得たベクトルを、平文データ中のｍバイトの所定数の要素分のベクトルとして平文データに格納する処理を、暗文データからのｍバイトの所定数の要素分のベクトルの読み出しごとに、上記乱数表の各段の表示位置を暗号化時と逆方向に１個ずつずらしながら繰り返すことによって、暗文の復号化を行うことを特徴としている。

【００１０】また、請求項５記載の発明は、共通鍵暗号化プログラムを記録した記憶媒体に係り、請求項１記載の共通鍵暗号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数のｍ次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データからｍバイトの文字列を取り出すごとに、上記乱数表と読み出し機構によって、上記（ｐ＋ｑ）個の原写像の番号の算出を行い、該（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号に示される原写像の合成写像を表す第１の間接指標配列と、前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号に示される原写像の合成写像を表す第２の間接指標配列とを作成して、上記平文データから取り出された文字列を上記第１の間接指標配列で変換し、次に該変換結果の文字列を上記定数係数のｍ次行列との積算で変換し、さらに該変換結果の文字列を上記第２の間接指標配列で変換して得た文字列を、暗文データ中のｍバイトの文字列として暗文データに格納する処理を、上記平文データからのｍバイトの文字列の読み出しごとに、上記乱数表の各段の表示位置を１個ずつずらしながら繰り返すことによって、平文の暗号化を行うプログラムを記録したことを特徴としている。

【００１１】また、請求項６記載の発明は、共通鍵復号化プログラムを記録した記憶媒体に係り、請求項２記載の共通鍵復号化方法を実行するプログラムを記録したコ

ンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数のｍ次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データからｍバイトの文字列を取り出すごとに、上記乱数表と読み出し機構によって、上記（ｐ＋ｑ）個の原写像の番号の算出を行い、該（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第１の間接指標配列と、前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号に示される原写像の暗号化時と逆順の配列の逆写像の合成写像を表す第２の間接指標配列とを作成して、上記暗文データから取り出された文字列を上記第２の間接指標配列で変換し、次に該変換結果の文字列を上記定数係数のｍ次行列の逆行列との積算で変換し、さらに該変換結果の文字列を上記第１の間接指標配列で変換して得た文字列を、平文データ中のｍバイトの文字列として平文データに格納する処理を、上記暗文データからのｍバイトの文字列の読み出しごとに、上記乱数表の各段の表示位置を暗号化時と逆方向に１個ずつずらしながら繰り返すことによって、暗文の復号化を行うプログラムを記録したことを特徴としている。

【００１２】また、請求項７記載の発明は、共通鍵暗号化プログラムを記録した記憶媒体に係り、請求項３記載の共通鍵暗号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像を表す間接指標配列と、定数係数のｍ次行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、平文データからｍバイトの所定数の要素分のベクトルを取り出すごとに、上記乱数表と読み出し機構によって、上記要素数回分の読み出しと上記（ｐ＋ｑ）個の原写像の番号の算出を行って、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号を第１の作業ベクトルに格納するとともに、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号を第２の作業ベクトルに格納し、上記平文データから取り出したベクトルの各要素を、上記第１の作業ベクトルの各要素に含まれる、上記ｐ個の原写像番号が指し示す原写像を用いて変換し、次に該変換結果のベクトルの各要素を上記定数係数のｍ次行列との積算で変換し、さらに該変換結果のベクトルの各要素を、上記第２の作業ベクトルの各要素に含まれる、上記ｑ個の原写像番号が指し示す原写像を用いて変換して得たベクトルを、暗文データ中のｍバイトの所定数の要素分のベクトルとして暗文データに格納する処理を、平文データからのｍバイトの所定数の要素分のベクトルの読み出しごとに、上記乱数表の各段の表示位置を１個ずつずらしながら繰り返すことによって、平文の暗号化を行うプログラムを記録したことを特徴としている。

【００１３】また、請求項８記載の発明は、共通鍵復号化プログラムを記録した記憶媒体に係り、請求項４記載の共通鍵復号化方法を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、長周期の乱数表と、該乱数表の表示値に基づき（ｐ＋ｑ）個の原写像番号を算出する読み出し機構と、それぞれの原写像の逆写像を表す間接指標配列と、定数係数のｍ次行列の逆行列とを予め用意し、秘密鍵を指定したとき、該秘密鍵から前記乱数表の表示開始位置を決定したのち、暗文データからｍバイトの所定数の要素分のベクトルを取り出すごとに、上記乱数表と読み出し機構によって、上記要素数回分の読み出しと上記（ｐ＋ｑ）個の原写像の番号の算出を行って、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｐ個の原写像番号を暗号化時と逆順に第１の作業ベクトルに格納するとともに、要素ごとに使用する前記（ｐ＋ｑ）個の原写像番号中のｑ個の原写像番号を暗号化時と逆順に第２の作業ベクトルに格納し、上記暗文データから取り出したベクトルの各要素を、上記第２の作業ベクトルの各要素に含まれる、上記ｑ個の原写像番号が指し示す原写像の逆写像を用いて変換し、次に該変換結果のベクトルの各要素を上記定数係数のｍ次行列の逆行列との積算で変換し、さらに該変換結果のベクトルの各要素を、上記第１の作業ベクトルの各要素に含まれる、上記ｐ個の原写像番号が指し示す原写像の逆写像を用いて変換して得たベクトルを、平文データ中のｍバイトの所定数の要素分のベクトルとして平文データに格納する処理を、暗文データからのｍバイトの所定数の要素分のベクトルの読み出しごとに、上記乱数表の各段の表示位置を暗号化時と逆方向に１個ずつずらしながら繰り返すことによって、暗文の復号化を行うプログラムを記録したことを特徴としている。

【００１４】

【作用】この発明の構成では、平文の暗号化を行う場合には、秘密鍵が与えられると、乱数表と読み出し機構の上での表示開始位置が定まる。次に、平文データから、平文データ中のｍバイト文字列を読み出す度に、乱数表と読み出し機構から値を読み出して、使用する（ｐ＋ｑ）個の原写像の番号を決定する。平文データ中のｍバイトの文字列は、まず原写像のｐ個の原写像番号の合成写像である間接指標配列によって変換され、次にｍ次の行列との積算によって変換され、最後に、原写像のｑ個の原写像番号の合成写像である間接指標配列によって変換されて、暗文データ中のｍバイトの文字列が生成される。逆に、暗文の復号化を行う場合には、秘密鍵が与えられると、乱数表と読み出し機構の上での表示開始位置が定まる。次に、暗文データから、暗文データ中のｍバ

イト文字列を読み出す度に、乱数表と読み出し機構から値を読み出して、使用する（ｐ＋ｑ）個の原写像の番号を決定する。暗文データ中のmバイト文字列は、まず原写像のｑ個の原写像番号の逆順の逆写像の合成写像である間接指標配列によって変換され、次にm次の行列の逆行列との積算によって変換され、最後に、原写像のｐ個の原写像番号の逆順の逆写像の合成写像である間接指標配列によって変換されて、平文データ中のmバイトの文字列が生成される。

【００１５】また、この発明の別の構成では、平文の暗号化を行う場合には、秘密鍵が与えられると、乱数表の上での表示開始位置が定まる。次に、平文データから、平文データ中のmバイト×所定要素数のベクトルを読み出す度に、乱数表と読み出し機構から値を読み出して、使用する（ｐ＋ｑ）個の原写像の番号を決定する。平文データ中のmバイト×所定要素数のベクトルは、まず要素ごとに使用するｐ個の原写像番号を格納した作業ベクトルの原写像を用いて変換（リストベクトルロード）され、次にm次の行列との積算によって変換され、最後に、要素ごとに使用するｑ個の原写像番号を格納した作業ベクトルの原写像を用いて変換（リストベクトルロード）されて、暗文データ中のmバイト×所定要素数のベクトルが生成される。逆に、暗文の復号化を行う場合には、秘密鍵が与えられると、乱数表の上での表示開始位置が定まる。次に、暗文データから、暗文データ中のmバイト×所定要素数のベクトルを読み出す度に、乱数表と読み出し機構から値を読み出して、使用する（ｐ＋ｑ）個の原写像の番号を決定する。暗文データ中のmバイト×所定要素数のベクトルは、まず要素ごとに使用するｑ個の原写像番号を、逆順に格納した作業ベクトルの逆写像を用いて変換（リストベクトルロード）され、次に、m次の逆行列との積算によって変換され、最後に、要素ごとに使用するｐ個の原写像番号を、逆順に格納した作業ベクトルの逆写像を用いて変換（リストベクトルロード）されて、平文データ中のmバイト×所定要素数のベクトルが生成される。

なお、剰余類の法、すなわち対象とする文字の種類の数が素数でない場合には、後述する定数係数行列の選択において、特別の注意が必要である。

【００２０】次に、この発明において用いられる間接指標配列による写像の仕組みについて説明する。図２は、この発明の実施の形態における間接指標配列による写像の仕組みについて示したものであって、（ａ）は指標と間接指標配列による写像の説明、（ｂ）は写像の例、（ｃ）は合成写像の例をそれぞれ示している。図２（ａ）に示すように、指標ｘを間接指標配列ｃ（ｊ）（ｊ＝０～８８）で変換すると、ｙ＝ｃ（ｘ）になる。指標配列ｘ（ｉ）（ｉ＝0～3）を、間接指標配列ｃ（ｊ）（ｊ＝０～８８）で変換すると、配列ｙ（ｉ）＝ｃ（ｘ（ｉ））になる。図２（ｂ）に示すように、指標配列（５０，６０，７０，８０）を、間接指標配列（２（０番），３，…，５２（５０番），…，６２（６０番），…，８８（８６番），０，１（８８番））で変換すると、配列（５２，６２，７２，８２）になる。また、図２（ｃ）に示すように、指標配列（５０，６０，７０，８０）を、間接指標配列（２（０番），３，…，５２（５０番），…，６２（６０番），…，８８（８６番），０，１（８８番））で変換し、さらに、間接指標配列（１（０番），２，３，…，５３（５２番），…，６３（６２番），…，８３（８２番），…，８８，０（８８番））で変換すると、配列（５３，６３，７３，８３）になる。

【００１６】したがって、この発明による暗文に対して、秘密鍵を知らずに解読を試みる者にとっては、既知平文攻撃から乱数表と読み出し機構の上の表示開始位置を知ることができない。また、既知の平文と暗文の組み合わせ、又は選択した平文と暗文の組み合わせから、差分をとって解析することもできない。また、選択平文攻撃を繰り返して、平文mバイトの総当たりを試行することも事実上できない。また、秘密鍵を総当たりで試行することもできない。また、間接指標配列を総当たりで試行することも、間接指標配列の原写像の順列の総当たりを試行することもできない。このように、この発明によれば、データを暗号化する場合に、長周期の乱数表と、乱数によって間接指標配列の順列を変化させる機構と、間接指標配列による変換で定数系列行列との積算を挟む形の合成写像とを用いることによって、既知平文攻撃並びに選択平文攻撃を、事実上不可能にすることができる。

【００１７】

【発明の実施の形態】最初に、この発明の実施の形態において用いられる写像の仕組みについて、図を参照しながら、簡単に説明する。

【００１８】近代以降の暗号においては、対象とする範囲の文字を、何らかの手法で数値と対応させることが必須である。対象とする文字の範囲は、前提とする通信路の種類によってさまざまである。また、文字と数値との対応のさせかたも、使用する暗号化の方式によっていろいろである。

【００１９】図１は、写像において、文字と数値を対応させる場合の例を示し、対象文字が８９種類の場合の、文字－数値間の対応を例示している。図１に示された例では、英字，数字，及びいくつかの記号を含む８９種類の文字を対象とした場合に、０～８８の整数値と対応させた例を示している。以降の説明においては、８９種類の文字を、８９を法とする剰余類の元と同一視するものとし、８９を法とする剰余類をＺ｜８９と表記する（式（１）参照）。

$$Z|89=\{0,1,\cdots,88\} \quad \cdots(1)$$

【００２１】この発明の実施の形態における以降の説明において、間接指標配列とは、Ｚ｜８９の元を１個ずつ任意の順序で配列したものである。すなわち、ｃ（ｊ）

$$\forall j \in Z|89$$

$$c(j) \in Z|89$$

$$\forall i, j \in Z|89$$

$$i \neq j \rightarrow c(i) \neq c(j)$$

間接指標配列は、１個の元又は任意の個数の元の配列を、別の文字で置き換える旨の、全単射の写像を表すことができる。変換される対象となる文字をｘとすると、当然、ｘ∈Ｚ｜８９である。これを間接指標配列ｃ（ｊ）で変換した写像の行き先は、ｃ（ｘ）である。間接指標配列は、何個かの元の配列を変換することもできる。例えば、変換される対象となる４個の文字の配列を、ｘ（ｉ）（ｉ＝0～3）とすると、当然、0≦ｉ≦3のそれぞれのｉについて、ｘ（ｉ）∈Ｚ｜８９である。これを間接指標配列ｃ（ｊ）で変換した写像の行き先は、ｃ（ｘ（ｉ））である。

【００２２】以降の説明では、変換される対象となる元又は元の配列を、指標又は指標配列と呼ぶ。これは、変換される対象の元が、間接指標配列の添字として、行き先を示す指標となっているためである。間接指標配列による写像の合成写像は、間接指標配列で表すことができる。間接指標配列ｃ１（ｊ），ｃ２（ｊ）（ｉ＝0～88）があったとき、指標ｘをまずｃ１（ｊ）で変換し、それからｃ２（ｊ）で変換した合成写像の行き先は、ｃ２（ｃ１（ｘ））である。ｃ１（ｊ）による変換に続いてｃ２（ｊ）による変換を行うという合成写像は、間接指標配列ｃ２（ｃ１（ｊ））で表される。

【００２３】図3は、この発明の実施の形態における間接指標配列による写像の逆写像について示したものであって、（ａ）は逆写像を表す間接指標配列の説明、（ｂ）は逆写像を表す間接指標配列の例をそれぞれ示している。

【００２４】図３（ａ）に示すように、指標配列ｘ（ｉ）（ｉ＝0～88）を間接指標配列ｃ（ｊ）（ｊ＝0～88）で変換して、配列（0，1，…，88）になる場合、配列ｘ（ｉ）（ｉ＝0～88）を間接指標配列とみなして表される写像は、配列ｃ（ｊ）の表す写像の逆写像である。

【００２５】図３（ｂ）に示すように、指標配列（87，88，0（2番），1，…，48（50番），…，58（60番），…，85（87番），86（88番））を、間接指標配列（2（0番），3，…，52（50番），…，62（60番），…，88（86番），0，1（88番））で変換すると、配列（0，1，2，…，87，88）になる。

【００２６】間接指標配列による写像には、必ず１個の逆写像が存在する。任意の間接指標配列ｃ（ｊ）（ｊ＝0～88）に対して、ただ１個の指標配列ｘ（ｊ）（ｊ＝0～88）が間接指標配列である場合は、式（２）及び式（３）に示す関係が成り立つ。

$$\cdots(2)$$

$$\cdots(3)$$

＝0～88）が存在し、ｃ（ｘ（ｊ））＝（0，1，…，88）となる。なぜならば、定義から、間接指標配列とは、Ｚ｜８９の元が１個ずつ並んだものだからである。（0，1，…，88）は、恒等写像であるから、上記の場合に、ｘ（ｊ）はｃ（ｊ）による変換の逆写像を表す間接指標配列である。

【００２７】図4は、この発明の実施の形態における行列の積算による写像の仕組みについて示したものであって、（ａ）は行列の積算による写像の説明、（ｂ）は行列の積算による写像の例をそれぞれ示している。図４（ａ）に示すように、指標配列ｘ（ｉ）（ｉ＝0～3）を、行列ｆ（ｉ，ｊ）（ｉ，ｊ＝0～3）との積算で変換すると、式（４）に示す配列が与えられる。

【００２８】

【数１】

$$y(i)=\sum_{j=0}^{3}(f(i,j)*x(j)) \qquad \cdots(4)$$

【００２９】図4（ｂ）に示すように、配列（1，2，3，4）を、式（５）に示す行列との積で変換すると、式（６）で表される指標配列（1，3，4，5）になる。

【００３０】

【数２】

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad \cdots(5)$$

【００３１】

【数３】

$$\begin{bmatrix} 1 \\ 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} \qquad \cdots(6)$$

【００３２】行列の積算による写像の仕組みは、次のようなものである。いま、ｘ（ｉ）はＺ｜８９の元を、いくつか並べた配列であって、例えば、４個の要素を持つ配列とする。４次の正方行列ｆ（ｉ，ｊ）（ｉ，ｊ＝0～3）があったとき、８９を法とする行列とベクトルとの積ｆｘは、Ｚ｜８９の元を４個並べた配列である。ｎ次の正方行列の積算は、Ｚ｜８９の元を４個並べた配列から、Ｚ｜８９の元を４個並べた配列への写像である。

【００３３】図5は、この発明の実施の形態における逆行列の積算による逆写像の仕組みについて示したもので

あって、（ａ）は逆行列の積算による逆写像の説明、（ｂ）は逆写像を表す逆行列の例をそれぞれ示している。図５（ａ）に示すように、行列ｇ（ｉ，ｊ）（ｉ，ｊ＝０～３）と、行列ｆ（ｉ，ｊ）（ｉ，ｊ＝０～３）との積が単位行列である場合、行列ｇとの積算による変換は、行列ｆとの積算による変換の逆写像である。図５（ｂ）及び式（７）に示すように、行列ｇと行列ｆとの積が単位行列である場合、

【００３４】

【数４】

$$\begin{pmatrix}1&0&0&0\\88&1&0&0\\88&0&1&0\\88&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0&0\\89&1&0&0\\89&0&1&0\\89&0&0&1\end{pmatrix}$$

$$\equiv_{(\mathrm{mod}\ 89)}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\quad\cdots(7)$$

【００３５】行列ｇとの積算による変換は、行列ｆとの積算による変換の逆写像である。逆行列の積算による逆写像の仕組みは、次のようなものである。いま、行列ｆに対して、逆行列ｇが存在したとき、行列ｇの積算による写像は、行列ｇの積算による写像の逆写像を表す。

【００３６】逆行列は、任意の行列ｆに対して常に存在するわけではない。特に、剰余類の法として素数でない数を選んだときは、注意が必要である。この発明の実施例では、定数係数の行列ｆと定数係数の逆行列ｇとの組み合わせを用いる。行列ｆに対して、逆行列が存在する場合、行列ｆは、Ｚ｜８９の元を４個並べた配列から、Ｚ｜８９の元を４個並べた配列への、全単射の写像である。

【００３７】以下、図面を参照して、この発明の実施の形態について説明する。説明は、実施例を用いて具体的に行う。

◇第１実施例

図６は、この発明の第１実施例である共通鍵暗号化又は復号化方法において、使用開始以前に決定し配布される事項を説明する図、図７，図８は、同実施例の方法における暗号化と復号化の手順を説明する図である。この例においては、図６に示す、乱数表と読み出し機構１と、原写像０～６７を表す間接指標配列２と、原写像０～６７の逆写像を表す間接指標配列３と、定数係数の４次行列ｆ４と、ｆの逆行列ｇ５とは、共通鍵暗号化又は復号化方法の使用開始以前に、別途決定され、配布されているものとする。

【００３８】乱数表と読み出し機構１は、ランダムな整数値を収容した１０段の乱数表を装備している。この乱数表の各段の長さは、順に、８９，８３，７９，…，４７のように、互いに素の関係になっている。読み出し機構は、適当な位置から読み出しを開始して、各段の現在の表示位置からそれぞれ１個の表示値を読み出し、１０種類の、各段の表示値の重み付き和ｂ１～ｂ１０を採取して、それぞれの重み付き和の、６８を法とする剰余ｃ１～ｃ１０を算出する。この場合の重みは適当に定めればよく、重みの種類ごとに重み付き和が求められる。読み出し機構は、１回の読み出しを行うごとに、各段における表示位置を１個ずつ右へずらしてゆく。この乱数表の周期は、Π（８９，８３，…，４７）であり、１．８×10^{18}程度である。原写像０～６７を表す間接指標配列２は、６８個の間接指標配列を並べたものである。各間接指標配列の内容は、適当な乱数を用いて作成することが望ましい。また、間接指標配列の数は、例えば後述のように、原写像の組み合わせの総当たりを試行する攻撃方法の場合と、乱数表の表示開始位置の総当たりを試行する攻撃方法の場合とで、試行回数と実行時間を勘案しながら、適当な値を選択すればよい。

【００３９】原写像０～６７の逆写像を表す間接指標配列３は、間接指標配列２の各配列に対して、それぞれの逆写像を表す間接指標配列を並べたものである。間接指標配列３を作成するためには、元数８９個のソートという操作を、６８回行うだけでよい。定数系列の４次行列ｆと、ｆの逆行例ｇは、逆行列が１個存在するように選ばれた、適当な行列である。定数系列の４次行列ｆには、単位行列を選んではならないのはもちろんだが、図５の（ｂ）に示されたような疎行列も好ましくなく、密行列を選ぶことが望ましい。また、行列の次数は、４次に限らず、例えば４次の倍数で任意に選ぶことができるが、この際、行列の次数と、１回の処理で取り扱う文字列のバイト数とが等しくなるようにすることが必要である。

【００４０】次に、図７，図８を用いて、この例の方法によって、平文の暗号化と、暗文の復号化とを行う場合の手順を説明する。まず、発信者に秘密鍵６を指定させることによって、この秘密鍵６から乱数表の各段の開始位置を決定する。秘密鍵６は、その長さを例えば８９種類の文字の内から指定する場合には、１０バイト以上を入力させることが推奨される。秘密鍵６から１０種類の任意の重みを付けた重み付き和ａ１～ａ１０を採取し、それぞれ８９を法とする剰余，８３を法とする剰余，…，４７を法とする剰余を算出して、乱数表の１段目，２段目，…，１０段目の表示開始位置を決定する（手順Ｓ１）。最初、平文データから、４バイトずつの文字列７を順次取り出し（手順Ｓ２）、文字列の取り出しごとに、乱数表と読み出し機構１から値を読み出して、使用

する原写像の番号ｃ１～ｃ５と、ｃ６～ｃ１０を決定する。

【００４１】次に、２に示す原写像０を表す間接指標配列～原写像６７を表す間接指標配列から、ｃ１番～ｃ５番の配列を取り出し、これらの合成写像を表す間接指標配列ｄ１を作成する（手順Ｓ３）。同様に、間接指標配列２から、ｃ６番～ｃ１０番の配列を取り出し、これらの合成写像を表す間接指標配列ｄ２を作成する（手順Ｓ４）。そして、平文データ中の４バイト文字列を、まず、間接指標配列ｄ１で変換し（手順Ｓ５）、次に変換結果の文字列を、行列ｆとの積算で変換し（手順Ｓ６）、さらにこの変換結果の文字列を、間接指標配列ｄ２で変換して（手順Ｓ７）、変換結果の文字列を暗文データ中の４バイト文字列８として格納する（手順Ｓ８）。次に、乱数表の各段の表示位置を１個ずつ右へ移動させ、平文データから次の４バイト文字列を読み出して、以下、上記と同様の処理を繰り返す。平文データの、４バイトに満たない終端部分の処理については、例えば、適当なデータをパディングして４バイトの倍数になるような調整を行えばよく、この発明の本質には無関係である。

【００４２】受信者が、このようにして生成された暗文の復号化を行う場合にも、上記の秘密鍵６を使用する。暗号化時と同様に、乱数表の各段の表示開始位置を決定する。暗文データから４バイトの文字列を取り出すごとに、暗号化の場合と同様に、原写像の番号ｃ１～ｃ１０を算出する。次に、３に示す原写像０の逆写像を表す間接指標配列～原写像６７の逆写像を表す間接指標配列から、ｃ１０番～ｃ６番の逆写像の配列を取り出し、これらの合成写像を表す間接指標配列ｅ２を作成する（手順Ｓ９）。この際、注意すべきことは、暗号化時には、ｃ６，ｃ７，…，ｃ１０の順に合成したのに対し、復号化時には、逆写像を、ｃ１０，ｃ９，…，ｃ６の順に合成する点である。

【００４３】次に、同様に、間接指標配列３からｃ５番～ｃ１番の逆写像の配列を取り出し、これらの合成写像を表す間接指標配列ｅ１を作成する（手順Ｓ１０）。この場合も、暗号化の場合とは逆の順序で合成することに注意する必要がある。なお手順Ｓ９と手順Ｓ１０は、どちらを先に行ってもよい。そして、暗文データ中の４バイト文字列８を、まず間接指標配列ｅ２で変換し手順Ｓ１１）、次に変換結果の文字列を、逆行列ｇとの積算で変換し（手順Ｓ１２）、さらにこの変換結果の文字列を、間接指標配列ｅ１で変換して（手順Ｓ１３）、変換結果の文字列を平文データ中の４バイト文字列として格納する（手順Ｓ１４）。暗文データの、４バイトに満たない終端部分の処理については、平文データの暗号化の場合と同様に処置すればよい。

【００４４】以下、この例の共通鍵暗号化方法による暗文に対して、秘密鍵を知らずに解読を試みた場合の、解読の可能性について検討する。いま、攻撃者が、暗号化の方法のうち、秘密鍵以外の部分、すなわち乱数表と読み出し機構１と、原写像０～６７を表す間接指標配列２と、原写像０～６７の逆写像を表す間接指標配列３と、定数係数の４次行列ｆ４と、ｆの逆行列ｇ５とを入手していると仮定すると、この場合、攻撃者は、秘密鍵６を知らないので、乱数表と読み出し機構１の上の表示開始位置を、直接には求められない。

【００４５】また、攻撃者が、例えば先頭の４バイトに関して、平文と暗文の組み合わせを入手したと仮定すると、この場合、原写像０～６７のうち、どれとどれがｃ１～ｃ１０として選ばれたかわからないため、間接指標配列ｄ１，ｄ２は、攻撃者にとって未知の写像である。ここで攻撃者が解くべき問題は、「既知の４バイトの文字列が、未知の間接指標配列ｄ１，既知の行列ｆとの積算，未知の間接指標配列ｄ２を経て、既知の４バイトの文字列となった場合の、間接指標配列ｄ１，ｄ２を求めよ。また、乱数表上の表示位置を求めよ。」ということになるが、この問題を解析的な手法で解くことはできない。

【００４６】また、攻撃者が、既知の平文と暗文の組み合わせ、又は、選択した平文と暗文の組み合わせから、差分をとって解析することを考えたと仮定すると、この発明の暗文は、間接指標配列による変換という、線形的な性質とは無縁の写像であって、行列の積算による変換を挟んだ形になっているので、差分解析は不可能である。

【００４７】また、攻撃者が、例えば先頭の４バイトに関して、平文と暗文の組み合わせを多数入手して、対応表を作ることで問題を解くことに代えようとしたと仮定すると、この場合は、単純に計算すれば、89^4　すなわち６千２百万個以上程度の組み合わせを入手しなければならない。既知平文攻撃とは、なんらかの事情で、平文が既知であるもののうち、相手側が同じ秘密鍵を用いて暗号化した暗文を入手できた場合に成立するものであるが、相手側が、６千２百万回も同じ秘密鍵を用いることを期待しても、それは、事実上不可能である。

【００４８】また、攻撃者が、以下のような選択平文攻撃を試みた場合を仮定する。すなわち、全文が一定の４バイトの文字列の繰り返しであるような平文データ、例えば、「ｃｏｍｐ」，「ｅｎｔｒ」，「ｃｏｎｃ」，「ｓｙｍｍ」，「ａｂｌｅ」，「ｔｈｅｎ」，「ｔｈａｎ」，「ｈｅｒｅ」等のような４バイトの文字列の繰り返しの平文データを作成する。そして、平文中に出現する頻度が高いと思われる文字列をつぎつぎに試行し、相手側に同じ秘密鍵で暗号化させて、暗文を入手する。また、同様に、上記の文字列が４バイトの整数倍の区切りに対して、１バイト，２バイト，又は３バイト目に出現した場合に相当する平文データを作成し、相手側に同じ秘密鍵で暗号化させて、暗文を入手する。

【００４９】つまり、出現する頻度が高いと思われる文字列１個につき、４通りの平文データを選択する。そして、対応表を作って目的の暗文と比較すれば、目的の暗文中の一定の位置に一定の文字列が出現した場合、当該位置の平文が判明する。ただし、この手法での攻撃を意味のあるものにするためには、どんなに少なくても、５０種類の文字列×４回程度以上の試行が必須と考えられる。選択平文攻撃とは、攻撃者が選択した平文を、なんらかの詐術を用いて、相手側に秘密鍵で暗号化させて、その暗文を入手することによって成立する。しかしながら、２００回以上もの選択平文攻撃を仕掛けられるなどということは、現実には考えられないことである。もしも、それが可能なほどの事情があるならば、秘密鍵を教えてもらうことのほうが、よほど簡単であろう。

【００５０】また、攻撃者が、乱数表と読み出し機構１を用い、表示開始位置の総当たりを試行したと仮定する。既述の通り、乱数表の周期は、１．８×10^{18}程度である。そこで、１秒間に１億回の試行を行うことが可能な計算機又は専用のハードウェアがあったとしても、この試行には、５７０年以上かかることになる。

【００５１】また、攻撃者が、秘密鍵の総当たりを試行したと仮定する。発信者が秘密鍵の長さとして１０バイトの文字列を用いていて、「１０バイト」という長さだけが既知であったとすると、可能な組み合わせは、３１×10^{18}程度である。そこで、１秒間に１億回の試行を行うことが可能な計算機又は専用のハードウェアがあったとしても、この試行には、９８００年以上かかることになる。

【００５２】また、攻撃者が、間接指標配列ｄ１，ｄ２の総当たりを試行したと仮定すると、８９の階乗は、１６×10^{135}　程度であるから、間接指標配列そのものの可能性をいちいち試すなどということは、絶対不可能なことである。そこで、原写像０～６７のうち、１０個のものが選ばれて合成されることから、可能な順列を総当たりで試行することになるが、可能な順列は$_{67}P_{10}$であって、２×10^{18}程度になり、上記の場合と同じ条件として、６００年以上かかることになる。

【００５３】この例の方法は、古典的な暗号化方式と比較すれば、「無限に近い長さの周期を持つ多表式暗号と、綴字換字暗号とを組み合わせたもの」に相当する。将来、計算機又は専用ハードウェアで実現できる実行速度が著しく改善され、上記各例で説明したような総当たりが可能になった場合には、乱数表の段数及び各段の幅と、合成写像に用いる間接指標配列の個数を定量的に増やすだけで対応でき、暗号化方式自体の定性的改変は必要とされない。

【００５４】このように、この例の共通鍵暗号化又は復号化方法によれば、長周期の乱数表と、乱数によって間接指標配列の順列を変化させる機構と、間接指標配列による変換で定数係数行列との積算を挟む形の合成写像とを有しているので、既知平文攻撃並びに選択平文攻撃を事実上不可能にすることができる。

【００５５】◇第２実施例

図９は、この発明の第２実施例である共通鍵暗号化又は復号化方法において、使用開始前に決定し配布される事項を説明する図、図１０，図１１は、同実施例の方法における暗号化と復号化の手順を説明する図である。この例においては、図９に示す、乱数表と読み出し機構１１と、原写像０～６７を表す間接指標配列１２と、原写像０～６７の逆写像を表す間接指標配列１３と、定数係数の４次行列ｆ１４と、ｆの逆行列ｇ１５とは、共通鍵暗号化又は復号化方法の使用開始前に、別途決定され、配布されているものとする。

【００５６】ここで、乱数表と読み出し機構１１，原写像０～６７を表す間接指標配列１２，原写像０～６７の逆写像を表す間接指標配列１３，定数係数の４次行列ｆ１４，ｆの逆行列ｇ１５は、それぞれ、図６に示された、乱数表と読み出し機構１，原写像０～６７を表す間接指標配列２，原写像０～６７の逆写像を表す間接指標配列３，定数係数の４次行列ｆ４，ｆの逆行列ｇ５と同様なので、以下、これらについての詳細な説明は省略する。

【００５７】次に、図１０，図１１を用いて、この例の方法によって、平文の暗号化と、暗文の復号化とを行う際の手順を説明する。まず、発信者に秘密鍵１６を指定させることによって、この秘密鍵１６から乱数表の各段の開始位置を決定する手順は、図７，図８に示された第１実施例の場合と同様である（手順Ｐ１）。最初、平文データから、４バイト×２５６要素のベクトル１７を取り出し（手順Ｐ２）、乱数表と読み出し機構１１から２５６回分の読み出しと、使用する原写像の番号ｃ１～ｃ１０の算出を行い、要素ごとに使用する原写像番号ｃ１～ｃ５を格納した作業ベクトル１８に格納し（手順Ｐ３）、要素ごとに使用する原写像番号ｃ６～ｃ１０を格納した作業ベクトル１９に格納する（手順Ｐ４）。なお、平文データから取り出すバイト数は、４バイトに限らないことは第１実施例の場合と同様であり、これと行列の次数との関係も同様である。また、要素数も２５６要素に限らず、例えば、５１２要素でもよい。

【００５８】次に、平文データ中の4バイト×２５６要素のベクトル１７の各要素を、要素ごとに使用する原写像番号ｃ１～ｃ５を格納した作業ベクトル１８の各要素に含まれる、ｃ１～ｃ５が指し示すところの原写像を用いて変換する（手順Ｐ５）。この操作はリストベクトルロードと呼ばれ、ベクトルパイプライン演算器を持つ計算機では、高速に実行できる。次に、上記の操作で得られたベクトルの各要素を、行列ｆとの積算で変換する（手順Ｐ６）。この操作は線形演算であり、ベクトルパイプライン演算器を持つ計算機では、高速に実行できる。次に、上記の操作で得られたベクトルの各要素を、

要素ごとに使用するｃ６～ｃ１０を格納した作業ベクトル１９の各要素に含まれる、原写像番号ｃ６～ｃ１０が指し示すところの原写像を用いて変換する（手順Ｐ７）。この操作は、上記と同様にリストベクトルロードであり、ベクトルパイプライン演算器を持つ計算機では、高速に実行できる。そして、変換結果のベクトルの各要素を、暗文データ中の４バイト×２５６要素のベクトルとして、暗文データ中に格納する（手順Ｐ８）。

【００５９】このようにして作成された暗文を復号化する際には、第１実施例の場合と同様に、逆写像，逆行列を用いて同様の手順によって行うことができる。暗号化時と同様に、乱数表の各段の表示開始位置を決定する。暗文データから４バイト×２５６要素のベクトル２０を取り出すごとに、乱数表と読み出し機構１１から２５６回分の読み出しと、使用する原写像の番号ｃ１～ｃ１０の算出を行って、要素ごとに使用する原写像番号ｃ１０～ｃ６を格納した作業ベクトル２１に格納し（手順Ｐ９）、要素ごとに使用する原写像番号ｃ５～ｃ１を格納した作業ベクトル２２に格納する（手順Ｐ１０）。なお、手順Ｐ９と手順Ｐ１０は、どちらを先に行ってもよい。

【００６０】次に、暗文データ中の４バイト×２５６要素のベクトル２０の各要素を、要素ごとに使用する原写像番号ｃ１０～ｃ６を格納した作業ベクトル２１の各要素に含まれる、ｃ１０～ｃ６が指し示すところの原写像の逆写像を用いて変換（リストベクトルロード）し（手順Ｐ１１）、変換結果の４バイト×２５６要素のベクトルの各要素を、行列ｆの逆行列ｇとの積算で変換（線形演算）し（手順Ｐ１２）、変換結果の４バイト×２５６要素のベクトルの各要素を、要素ごとに使用する原写像番号ｃ５～ｃ１を格納した作業ベクトル２２の各要素に含まれる、ｃ５～ｃ１が指し示すところの原写像の逆写像を用いて変換（リストベクトルロード）して（手順Ｐ１３）、変換結果の４バイト×２５６要素のベクトルを平文データ中の４ハイト×２５６要素のベクトルとして、平文データに格納する（手順Ｐ１４）。暗文データの、４バイトに満たない終端部分の処理については、平文データの暗号化の場合と同様に処置すればよい。

【００６１】このように、この例の共通鍵暗号化方法によれば、長周期の乱数表と、乱数によって間接指標配列の順列を変化させる機構と、間接指標配列による変換で定数係数行列との積算を挟む形の合成写像とを有しているので、既知平文攻撃並びに選択平文攻撃を事実上不可能にすることができる。

【００６２】この例の共通鍵暗号化方法による暗文に対しても、既知平文攻撃並びに選択平文攻撃が事実上不可能である。その理由は、第１実施例について説明したのと同様なので、詳細な説明は省略する。

【００６３】以上、この発明の実施例を図面により詳述してきたが、具体的な構成はこの実施例に限られたものではなく、この発明の要旨を逸脱しない範囲の設計の変更等があってもこの発明に含まれる。例えば、この発明をソフトウェアによって実現する場合は、ハードウェアとして、汎用機，ワークステーション，パーソナルコンピュータ等、適当なコンピュータシステムを備え、これにこの発明の方法を実行するためのプログラムを装備することによって容易に実現できる。さらに、このようなプログラムを、処理装置が読み取り可能な、任意の形式の媒体に記録した状態で予め用意することによって、同様なシステムを具備する場合に、同一の方法を普遍的に実現することができる。

【００６４】

【発明の効果】以上説明したように、この発明によれば、長周期の乱数表と、乱数により間接指標配列の順序を変化させる機構と、間接指標配列による変換で定数係数との積算を挟む形の合成写像とを有しているので、既知平文攻撃並びに選択平文攻撃を事実上不可能とする、共通化鍵暗号化又は復号化方法を実現するとともに、共通鍵暗号化又は復号化プログラムを記録した記憶媒体を提供することができる。

【図面の簡単な説明】

【図１】写像において、文字と数値を対応させる場合の例を示す図である。

【図２】この発明の一実施の形態における間接指標配列による写像の仕組みについて示す図である。

【図３】同実施の形態における間接指標配列による写像の逆写像について示すための図である。

【図４】同実施の形態における行列の積算による写像の仕組みについて示すための図である。

【図５】同実施の形態における逆行列の積算による逆写像の仕組みについて示すための図である。

【図６】この発明の第１実施例である共通鍵暗号化又は復号化方法において、使用開始以前に決定し配布される事項を説明する図である。

【図７】同実施例の方法における暗号化と復号化の手順を説明する図である。

【図８】同実施例の方法における暗号化と復号化の手順を説明する図である。

【図９】この発明の第２実施例である共通鍵暗号化又は復号化方法において、使用開始前に決定し配布される事項を説明する図である。

【図１０】同実施例の方法における暗号化と復号化の手順を説明する図である。

【図１１】同実施例の方法における暗号化と復号化の手順を説明する図である。

【符号の説明】

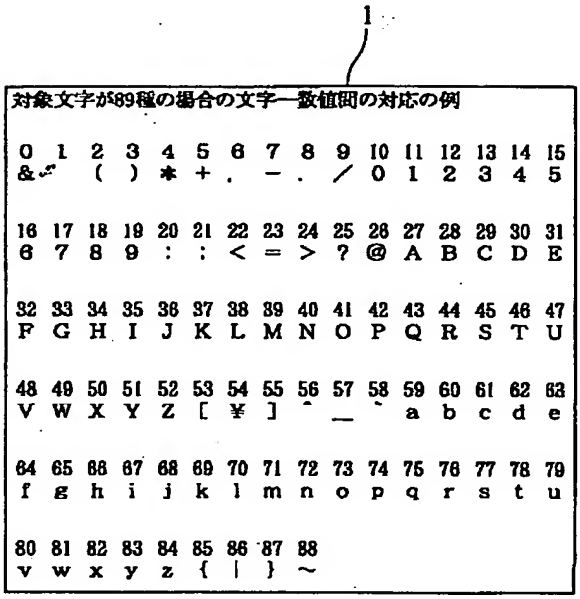
１，１１　乱数表と読み出し機構

２，１２　原写像０～６７を表す間接指標配列

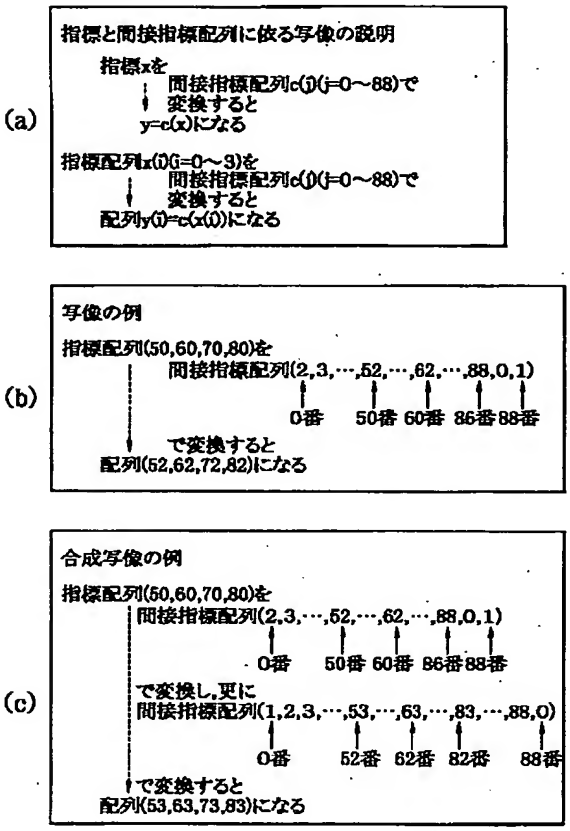
３，１３　原写像０～６７の逆写像を表す間接指標配列

4，14　定数係数の4次行列
5，15　定数係数の4次行列の逆行列
6，16　秘密鍵
7　平文データ中の4バイト文字列
8　暗文データ中の4バイト文字列
17　平文データ中の4バイト×256要素のベクトル
20　暗文データ中の4バイト×256要素のベクトル

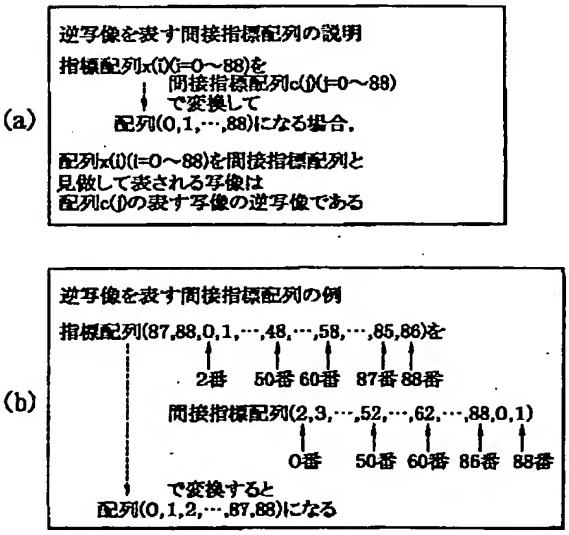
【図1】



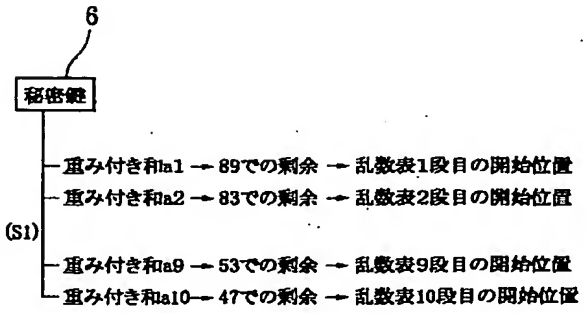
【図2】



【図3】



【図7】



【図4】

(a)

行列の積算に依る写像の説明

配列x(i)(i=0～3)を
行列f(i,j)(i,j=0～3)との
積算で変換すると

配列 $y(i)=\sum_{j=0}^{3}(f(i,j)*x(j))$

になる

(b)

行列の積算に依る写像の例

配列(1,2,3,4)を

行列 $\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}$ との

積算で変換すると

$$\begin{pmatrix}1\\3\\4\\5\end{pmatrix}=\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}\begin{pmatrix}1\\2\\3\\4\end{pmatrix}$$

配列(1,3,4,5)になる

【図5】

(a)

逆行列の積算に依る逆写像の説明

行列g(i,j)(i,j=0～3)と
行列f(i,j)(i,j=0～3)との積が
単位行列である場合、

行列gとの積算による変換は
行列fとの積算による変換の
逆写像である。

(b)

逆写像を表す逆行列の例

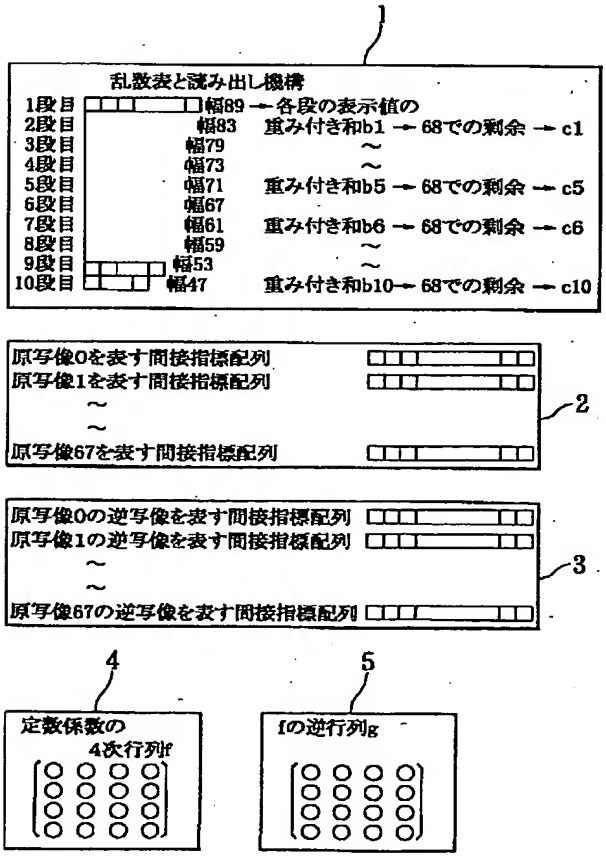
行列g と 行列f との積が 単位行列

$$\begin{pmatrix}1&0&0&0\\88&1&0&0\\88&0&1&0\\88&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0&0\\89&1&0&0\\89&0&1&0\\89&0&0&1\end{pmatrix}$$

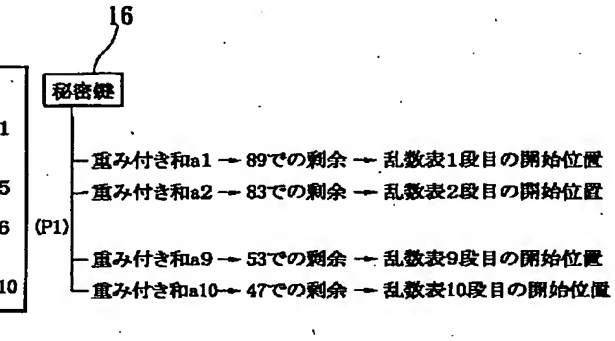
$$=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\pmod{89}$$

行列gとの積算による変換は
行列fとの積算による変換の
逆写像である。

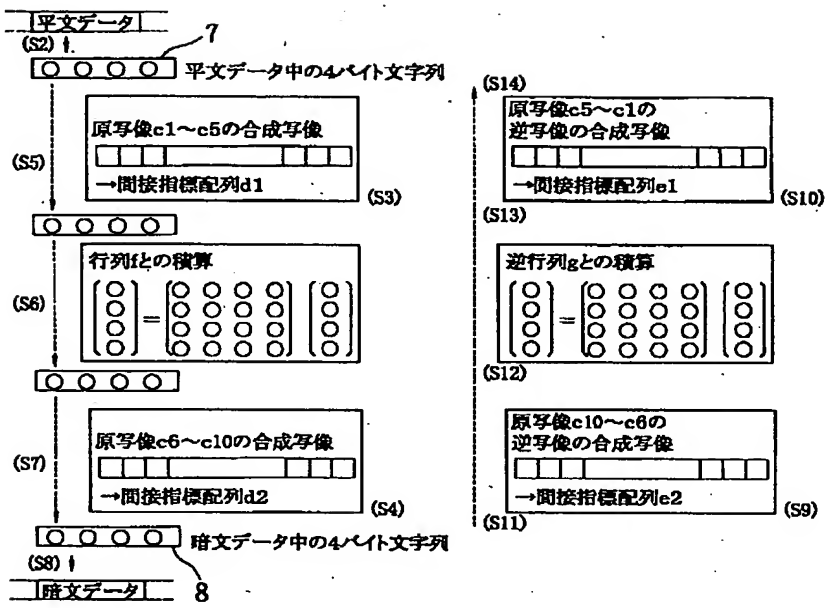
【図6】



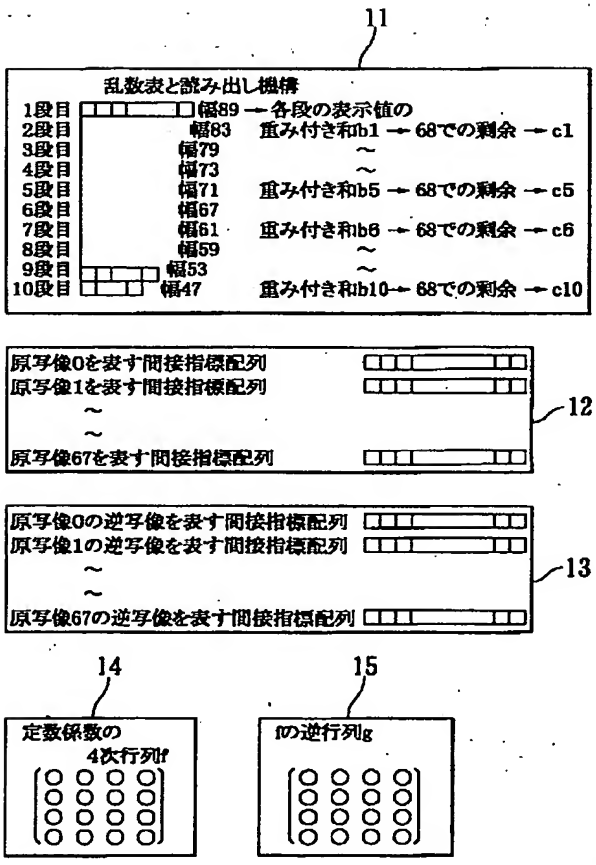
【図10】



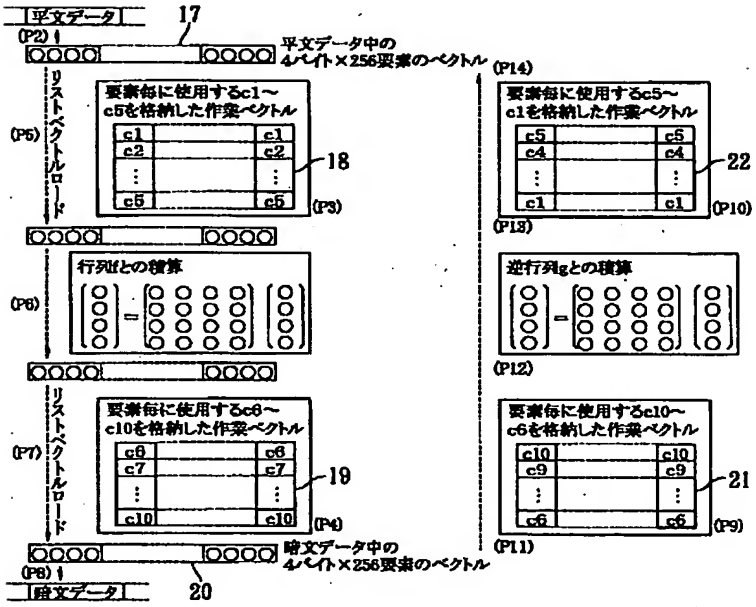
【図8】


平文データ
(S2)
7
平文データ中の4バイト文字列
原写像c1～c5の合成写像
→間接指標配列d1
(S3)
(S5)
行列fとの積算
(S6)
原写像c6～c10の合成写像
→間接指標配列d2
(S4)
(S7)
暗文データ中の4バイト文字列
(S8)
暗文データ
8
(S14)
原写像c5～c1の
逆写像の合成写像
→間接指標配列e1
(S10)
(S13)
逆行列gとの積算
(S12)
原写像c10～c6の
逆写像の合成写像
→間接指標配列e2
(S9)
(S11)

【図9】


11
乱数表と読み出し機構
1段目 幅89 → 各段の表示値の
2段目 幅83 重み付き和b1 → 68での剰余 → c1
3段目 幅79
4段目 幅73
5段目 幅71 重み付き和b5 → 68での剰余 → c5
6段目 幅67
7段目 幅61 重み付き和b6 → 68での剰余 → c6
8段目 幅59
9段目 幅53
10段目 幅47 重み付き和b10 → 68での剰余 → c10
原写像0を表す間接指標配列
原写像1を表す間接指標配列
原写像67を表す間接指標配列
12
原写像0の逆写像を表す間接指標配列
原写像1の逆写像を表す間接指標配列
原写像67の逆写像を表す間接指標配列
13
14
定数係数の
4次行列f
15
fの逆行列g

【図11】


平文データ
17
(P2)
平文データ中の
4バイト×256要素のベクトル
(P14)
リストベクトルロード
(P5)
要素毎に使用するc1～
c5を格納した作業ベクトル
c1
c2
c5
18
(P3)
要素毎に使用するc5～
c1を格納した作業ベクトル
c5
c4
c1
22
(P10)
(P13)
行列fとの積算
(P6)
逆行列gとの積算
(P12)
リストベクトルロード
(P7)
要素毎に使用するc6～
c10を格納した作業ベクトル
c6
c7
c10
19
(P4)
要素毎に使用するc10～
c6を格納した作業ベクトル
c10
c9
c6
21
(P9)
(P11)
暗文データ中の
4バイト×256要素のベクトル
(P8)
暗文データ
20